AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A memory protection system comprising:

a key store to store ~~storing~~ identifiers of protected memory locations and respective corresponding memory protection keys; and

a memory access manager including at least hardware configured to:

receive a memory command for altering contents of any of the protected memory locations,

determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, wherein the memory protection key in the memory command is written to a volatile memory,

if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and

then render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory command.

2. (Original) The system of claim 1, wherein the identifiers comprise addresses in a protected memory.

3. (Original) The system of claim 1, wherein the identifiers comprise names of protected files in a memory.

4. (Original) The system of claim 1, wherein the identifiers identify data entries in a protected memory.

5. (Original) The system of claim 1, wherein each of the memory protection keys comprises a modified version of a data sequence.

6. (Original) The system of claim 5, wherein the modified version comprises a hash of the data sequence.

7. (Original) The system of claim 1, wherein the key store stores a mapping table that maps each identifier to a corresponding memory protection key.

8. (Original) The system of claim 7, wherein at least one of the identifiers is mapped to multiple corresponding memory protection keys.

9. (Original) The system of claim 1, implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations.

10. (Previously Presented) The system of claim 9, wherein the memory access manager is further configured to receive memory commands for altering contents of the unprotected memory locations, and to permit the memory commands for altering contents of the unprotected memory locations without checking for any memory protection key.

11. (Previously Presented) The system of claim 1, wherein the memory access manager is further configured to perform the memory command that includes the memory protection key corresponding to each protected memory location to be altered.

12. (Previously Presented) The system of claim 1, implemented in an electronic device, wherein the memory command is received by the memory access manager from an originating electronic device component, and wherein the originating electronic device component proceeds with the memory command permitted by the memory access manager.

13. (Original) The system of claim 12, wherein the originating electronic device component is a memory update module.

14. (Original) The system of claim 12, wherein the originating electronic device component sends memory commands to the memory access manager responsive to data received at the electronic device.

15. (Original) The system of claim 14, wherein the originating electronic device component is further configured to extract a received memory protection key from the received data and to provide the received memory protection key to the memory access manager.

16. (Previously Presented) An electronic device comprising:

a memory;

a wireless receiver configured to receive data relating to a remote software update to be written to the memory;

a memory protection system associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location; and

volatile storage having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations, and the memory protection system to render the key inaccessible by overwriting at least a portion of the key.

17. (Previously Presented) The electronic device of claim 16, wherein the volatile storage is part of the memory.

18. (Cancelled)

19. (Previously Presented) The electronic device of claim 16, wherein the memory protection system comprises:

a key store storing a mapping table that associates the protected memory locations with the respective corresponding keys; and

a memory access manager configured to:

process a memory command for writing the received data to any of the protected memory locations,

determine whether the received data includes the key corresponding to any of the protected memory locations to which the received data is to be written,

if the received data includes the key corresponding to a protected memory location to which the received data is to be written,

permit the memory command to proceed, and

then render the corresponding key in the received data inaccessible.

20. (Original) The electronic device of claim 19, wherein the memory comprises a file system, and wherein the key store resides at a secure location in the memory outside the file system.

21. (Cancelled)

22. (Currently Amended) A method of protecting memory in an electronic device, comprising:

receiving a memory command to access a protected memory location;

determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location;

in response to determining that the received memory command is the memory write command:

identifying a memory protection key corresponding to the protected memory location;

determining whether the memory write command includes the memory protection key corresponding to the protected memory location, wherein at least the memory protection key in the memory write command has been written to volatile memory;

permitting completion of the memory write command if the memory write command includes the memory protection key corresponding to the protected memory location; and

rendering the memory protection key in the memory write command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command; and

in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key.

23. (Previously Presented) The method of claim 22, wherein permitting comprises performing the memory write command.

24. (Previously Presented) The method of claim 22, wherein receiving comprises receiving the memory command from an originating electronic device component, and wherein permitting

comprises allowing the originating electronic device component to perform the memory write command.

25. (Previously Presented) The method of claim 22, further comprising:
receiving data to be written to the protected memory location; and
generating the memory write command responsive to receiving the data.

26. (Previously Presented) The method of claim 44, wherein the received data comprises a received key, and wherein generating comprises extracting the received key from the received data and inserting the received key into the memory write command.

27. (Previously Presented) The method of claim 26, wherein determining comprises comparing the memory protection key corresponding to the protected memory location with the received key in the memory write command.

28. (Previously Presented) The method of claim 26, wherein determining comprises retrieving a modified version of the memory protection key corresponding to the protected memory location, modifying the received key in the memory write command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location.

29. (Cancelled)

30. (Previously Presented) The method of claim 22, wherein identifying comprises identifying a protected memory location in the memory write command and accessing a mapping table that maps protected memory locations to respective corresponding memory protection keys.

31. (Cancelled)

32. (Previously Presented) The method of claim 22, further comprising:

receiving memory commands to alter unprotected memory locations; and

permitting completion of the memory commands to alter unprotected memory locations without checking for any memory protection keys.

33. (Cancelled)

34. (Original) The method of claim 22, wherein said identifying step comprises accessing the memory protection key corresponding to the protected memory location in a key store, the method further comprising:

receiving a command to establish a new protected memory location in the memory and a memory protection key corresponding to the new protected memory location;

establishing the new protected memory location in the memory; and

storing the memory protection key in the key store.

35. (Original) A computer-readable medium storing instructions for performing the method of claim 22.

36. (Currently Amended) A method of protecting electronic memory, comprising:

configuring a memory store of an electronic device into at least one protected memory location and a key store operable to store an identifier of each protected memory location and a respective corresponding memory protection key; and

configuring a processor of the electronic device to provide a memory access manager operable to receive memory commands for altering contents of any of the at least one protected memory location, and for at least one memory command, to:

determine whether the at least one memory command includes a memory protection key corresponding to at least one protected memory location to be modified, said at least one memory command including the memory protection key corresponding to at least one said protected memory location to be modified, [[to]]

permit the at least one memory command to complete, and

then render each corresponding memory protection key in the at least one memory command inaccessible by overwriting at least a portion of the memory protection key upon completion of the at least one memory command, wherein the at least one memory command corresponds to a remote software update received by a wireless receiver for updating the at least one protected memory location to be modified.

37. – 38. (Cancelled)

39. (Original) A computer-readable medium storing instructions for performing the method of claim 36.

40. (Cancelled)

41. (Previously Presented) The system of claim 1, wherein the memory access manager is configured to further receive a memory read command to read content of a particular protected memory location, the memory access manager to allow the memory read command to proceed to read the content of the particular protected memory location without checking for any memory protection key.

42. (Cancelled)

43. (Previously Presented) The electronic device of claim 16, wherein the memory protection system is configured to further:

receive a memory read command to access a particular one of the protected memory locations,

perform reading of the particular protected memory location in response to the memory read command, without checking for any memory protection key.

44. (Previously Presented) The method of claim 25, wherein receiving the data to be written comprises receiving, by a wireless receiver, a remote software update to be written to the protected memory location.

45. (Previously Presented) The method of claim 36, wherein configuring the processor further comprises configuring the processor to receive a memory read command to read a particular one of the protected memory locations, and to permit the memory read command to read the particular protected memory location without checking for any memory protection key.

46. (Previously Presented) The memory protection system of claim 1, wherein the at least a portion of the memory protection key is overwritten upon completion of the memory command.

47. (New) The method of claim 36, wherein the memory protection key in the at least one memory command is written to volatile memory, and wherein the memory protection key in the at least one memory command is rendered inaccessible by overwriting at least the portion of the memory protection key written to the volatile memory such that the memory protection key written to the volatile memory is rendered inaccessible after completion of the at least one memory command.